Public Comments Received Regarding Law Harmonization Recommendations

This document is a compilation of all public comments received following the Law Harmonization Public Forum on July 9, 2012. The written comments from each commenter are copied to this document, minus any header (address) and/or signature information. The purpose of this working document is to facilitate responses to the public comments by the Privacy Steering Team and CalOHII. The complete text of each public comment can be found on the CalOHII website, http://ohii.ca.gov/calohi/eHealthPolicy/PrivacySteeringTeam.aspx

PUBLIC COMMENTS

California Association of Marriage and Family Therapists

On behalf of the thirty-thousand members of the California Association of Marriage and Family Therapists, we welcome the opportunity to provide CalOHII with comments concerning the harmonization of HIPAA and CMIA. Although we are generally in favor of harmonizing these laws, which should help make compliance efforts less costly and less confusing for providers, we encourage CalOHII to adopt the most stringent laws possible to protect the confidentiality of mental health information. Towards that end, we have three suggestions.

Our first suggestion is for CalOHII to remember that not all health care providers are "covered providers" under HIPAA, and are therefore subject to CMIA only while practicing in California. Many of our members are not "covered providers" under HIPAA because they operate their practices on a cash-only basis. Many others interact with insurance companies and managed care organizations through the mail or telephone only. In reviewing CalOHII's "Privacy and Security Steering Team Law Harmonization Recommendations," however, some of the recommendations call for parts of HIPAA to be adopted and parts of CMIA to be removed. This may create unforeseen problems for health care professionals in California who do not conduct electronic transactions. As CalOHII works through the harmonization process, we believe it is important to keep in mind that the resulting law must be flexible enough to cover the workings of health care professionals who *do* conduct electronic transactions as well as those who *do not* conduct such transactions. Ultimately, though, we believe it is in the best interests of providers to have a more unified law and not two separate systems.

Our second suggestion concerns heightening the protection of mental health information. In addressing the subject of mental health records, CMIA and HIPAA treat the subject differently. Under CMIA, mental health records are a subset of "medical information" (California Civil Code § 56.05(g)). However, HIPAA recognizes a separate and distinct category of "health information" called "psychotherapy notes" (45 C.F.R. § 164.501). We would encourage CalOHII to adopt not only the definition of "psychotherapy notes" set forth in 45 C.F.R. § 164.501, but also the limitations on uses and disclosures of "psychotherapy notes" set forth in 45 C.F.R. §164.508. Incorporating HIPAA's concept of "psychotherapy notes" into CMIA would likely help ease concerns of patients regarding the "confidentiality" of their mental health information.

Our third suggestion is amending California Civil Code § 56.104 ("CC § 56.104") to bring it into harmony with HIPAA and its fundamental concepts of "minimum necessary" and "psychotherapy notes." A problem with CC § 56.104 is that it allows third parties to access outpatient psychotherapy records without patients authorizing such disclosures, or even being aware that their psychotherapists have made such disclosures, which is inimical to the therapeutic process. Under CC § 56.104 a third party who has accessed outpatient psychotherapy records only has to provide patients with written notification of such access within thirty days of receiving the outpatient psychotherapy records. We believe CC § 56.104 is anachronistic, in light of HIPAA's enactment, because the statute allows third parties unfettered access to outpatient psychotherapy records, which conflicts with HIPAA's fundamental concepts of "minimum necessary" and "psychotherapy notes."

In our view, consumers of mental health services need to know that their mental health information will be kept confidential. As the Court of Appeal, 4th District recognized in *San Diego Trolley, Inc. v. Sup. Ct.* (2001) 97 Cal.App.4th 1083, “Psychoanalysis and psychotherapy are dependent upon the fullest revelation of the most intimate and embarrassing details of the patient’s life. Unless a patient is assured that such information can and will be held in utmost confidence, he or she will be reluctant to make the full disclosure upon which diagnosis and treatment depends.”

Confidentiality and trust are key ingredients of the "glue" that holds the psychotherapist-patient relationship together, and unwarranted or excessive intrusions into patient confidences erodes this glue. Consequently, as CalOHII works to harmonize HIPAA and CMIA, we urge it to adopt the most stringent laws possible concerning the confidentiality of mental health information.

Thank you for your attention to this matter, and we welcome any questions regarding these issues.

Public Comments Received Regarding Law Harmonization Recommendations

California Hospital Association

The California Hospital Association (CHA) is a nonprofit organization dedicated to representing the interests of California hospitals and the patients they serve. CHA has more than 400 hospital and health system members, including general acute care hospitals, children's hospitals, rural hospitals, psychiatric hospitals, academic medical centers, county hospitals, investor-owned hospitals, and multi-hospital health systems. These hospitals furnish vital health care services to millions of our states' citizens. CHA provides its members with state and federal representation in the legislative, judicial, and regulatory arenas, in an effort to improve health care quality, access and coverage; promote health care reform and integration; achieve adequate health care funding and contain costs; improve and update laws and regulations; and maintain public trust in health care.

CHA supports the effort to harmonize state and federal health information privacy laws, and appreciates the complex undertaking and diligent work of the CalOHII Privacy and Security Steering Team. CHA recognizes that it is not a quick or easy job to compare state and federal privacy provisions and analyze the effects of the differences. CHA wholeheartedly agrees that minimizing the differences between state and federal law will allow patients as well as health care providers to better understand and follow the laws, and will reduce the costs of compliance – in other words, harmonization will lead to better quality of care at a lower cost.

CHA appreciates the opportunity to comment on the CalOHII Privacy and Security Steering Team Law Harmonization Recommendations. We address the two major concepts in the recommendations: revising the definition of terms in California law to match HIPAA definitions, and importing HIPAA provisions into California law.

Definitions of Terms

To the extent that the California Confidentiality of Medical Information Act (CMIA) and the Health Insurance Portability and Accountability Act (HIPAA) regulations use the same (or a similar) term, but define it differently, CHA supports revising the CMIA by using exact HIPAA definitions and making other corresponding revisions. (For example: line 21, "group health plan"; line 26, "health care provider"; line 27, "health information" instead of "medical information"; line 39, "marketing.") Harmonizing terms will help everyone (patients, providers, payers, enforcement agencies) understand – and thus comply with – this complicated area of law.

In addition, CHA notes that the CMIA generally prohibits the "sale" of medical information without patient authorization (Civil Code Section 56.10(d)), but does not define the term "sale." HIPAA also prohibits the sale of protected health information (PHI), but excludes certain transactions (42 U.S.C. Section 17935(d)). CHA supports aligning the two definitions. (Note: the Secretary of the U.S. Health and Human Services Agency (HHS) was required to promulgate regulations by Aug. 18, 2010 to carry out this provision of the HITECH Act. She has not yet done so.)

Incorporating HIPAA Regulation Language into California Law

The CalOHII Privacy and Security Steering Team Law Harmonization Recommendations support the concept of writing the HIPAA regulation language into California law (into the CMIA). CHA strongly opposes this concept.

Adding HIPAA language to California law will have the following negative repercussions:

1. **Differing Standards.** The major goal of the CalOHII Privacy and Security Steering Team is to "harmonize" state and federal law. However, if the HIPAA standards are written into the CMIA, it is inevitable that eventually either HIPAA or the CMIA (or both) will be revised, and the standards will again differ. If the HIPAA standards are referenced in California law (rather than written into California law word-by-word), a specific version of the regulations would need to be referenced to prevent a potential constitutional problem regarding a legislative delegation of authority. It is unrealistic to expect that HIPAA and CMIA will thereafter stay static - indeed, we are currently waiting for the Office of Management and Budget to release revised HIPAA regulations.

At the public hearing on July 9, one of the CalOHII Privacy and Security Steering Team panelists indicated that many California entities that are covered by CMIA are not covered by HIPAA. He indicated that this was the concern driving the proposal to write HIPAA into the CMIA. HIIPAA covers all health plans, all clearinghouses, any health care provider that transmits health information in electronic form in connection with a standard transaction (such as electronic billing, payment or eligibility verification), as well as any business associate of such entities. (See 45 C.F.R. Sections 160.103 and 42 U.S.C. Sections 17931 and 17934.) To my knowledge, the main California entities that are covered by CMIA but not by HIPAA are cash/check-based health care providers that do not undertake electronic transactions, such as dermatologists whose primary practice consists of cosmetic procedures and psychotherapists who do not accept private insurance or government payments. If the CalOHII Privacy and Security Steering Team wishes to

address this problem in California law, CHA would not object to a narrow, targeted fix.

2. **Duplicative Enforcement and Penalties**. If HIPAA language is written into the CMIA, California health care providers and payers (including state and local government agencies) would become subject to state enforcement of federal requirements. Currently, the federal Office for Civil Rights (OCR, which is part of HHS) is the lead enforcement agency for HIPAA privacy and security compliance. California taxpayers should not be asked to fund additional government employees to enforce HIPAA, and California providers and payers should not be asked to undergo additional investigations and audits by an entirely different government agency. This would likely lead to differing interpretations of the same language, and would subject California entities to both state penalties and federal penalties for the same violation.

3. **Private Cause of Action**. The HIPAA privacy and security standards explicitly are not subject to a private cause of action. The federal government made a deliberate decision that individuals should bring any complaint about HIPAA violations to OCR rather than to court. OCR will investigate and either educate or penalize the violator as appropriate. If HIPAA regulatory language is inserted into California law, then patients and their lawyers will be able to sue in court over a violation. Health care providers and payers will be forced to divert money away from providing high-quality patient care to paying legal bills.

Thank you for considering CHA's comments. CHA believes that the CalOHII Privacy and Security Team's goals can be achieved, and the problems described above can be eliminated, through careful legislative drafting. I would like to reiterate CHA's willingness – indeed, eagerness - to assist the CalOHII Privacy and Security Steering Team as this project progresses. In addition, CHA understands that the CalOHII Privacy and Security Steering Team has decided not to address the privacy provisions in the Lanterman- Petris-Short Act at this time; we look forward to working with you regarding those laws in the future so as not to impede the integration efforts underway in the mental health and physical health delivery systems.

Public Comments Received Regarding Law Harmonization Recommendations

Clinical Informatics

Clinical Informatics is pleased to be able to respond to the recently released document harmonizing CMIA and HIPAA representing the valuable efforts of the multi-stakeholder Privacy and Security Steering Teams. This effort is phenomenal in its scope and impressive in its result. We applaud everyone who participated in the process. Overall, we agree with the majority of the findings and recommendations and wish to focus only on those few areas of disagreement or where there may be value in reconsideration or additional clarity.

On page 5, number 12, there is a limited definition of data aggregation. There is a potential problem with adopting this definition. Data aggregation as a concept includes aggregation of data from multiple individuals, regardless of whether one or more CE is involved. If the new definition only applies to BAs, what new term or terms should we define to refer to data aggregation within a single CE (e.g. a hospital that aggregates its patient data for internal study or review)or by a BA in reference to a single CE? Perhaps the definition as proposed should be broadened.

On page 5, number 16, it is unclear what this section is resolving. HIPAA applies to data in motion and at rest, not the specific technology being used. Could an example be provided of a technology that is excluded from the current HIPAA definition? If not, perhaps this section is unnecessary.

On page 14, number 57, the comment is unclear. Is the comment suggesting that additional definitions should be created for care management and care coordination?

On page 28, number 105, are these access controls intended for entities to manage their employees or is it intended to apply to all access to PHI, such as by patients or care givers? The implications and expense will be markedly different.

On page 30, number 109, the new rule should focus on a proper balance. HIPAA generally requires that an entity take reasonable measures to reduce risks and protect PHI. HIPAA does not require the same level of investment by all entities, but considers entity size and the resources each has available. In the absence of an explicit HIPAA requirement for NIST CMVP, this rule should be markedly reduced in its scope. As written, its expense in time and resources are likely to create a barrier for small provider practices. At a minimum, this item should be reassessed.

Thank you again for the opportunity to participate in this well managed and very important process. I look forward to continued participation in the process. As HIPAA changes over time, it is likely that this type of review will be necessary on a periodic basis.

Public Comments Received Regarding Law Harmonization Recommendations

Consumer Watchdog

I am writing on behalf of Consumer Watchdog to express our concern about the current effort to "harmonize" the California Confidentiality of Medical Information Act and the federal Health Insurance Portability and Accountability Act. As we understand the process, the goal is to use HIPAA as the "floor" to protect our medical privacy, but in those areas where the CMIA provides greater protections, California state law would prevail. As the background document from CalOHII puts it, "the consensus among stakeholders is to take HIPAA rules as the base and augment with CMIA where necessary or desirable." Put another way, the goal of the harmonization effort should be to preserve the current relationship between federal and state law.
The effort must not weaken current California privacy protections. Harmonization must follow the basic medial dictum, "First, do no harm."

Unfortunately CalOHII has offered no way to tell whether this is the case. You have released a document, "Privacy and Security Team Law Harmonization Recommendations." Frankly this document is incomprehensible. It is simply a list of terms followed by the recommendation to adopt a definition – usually from HIPAA. There is no analysis of how CMIA definitions differ from HIPAA definitions or explanation of why the recommendations were made. Put simply, you need to show your work. This document does not offer and adequate explanation of what is at stake in the recommendations about these legal provisions, and why the Privacy Steering Team made them. Medical privacy is a critical issue to the public. You must not exclude the public from participating because we aren't provided with adequate information to understand the issues. People should have access to all analyses and information on which these decisions were based, so that they can understand what the proposed harmonization will do. The document provided is completely inadequate for that purpose.

The document says "the goal of the current vetting of these recommendations is to determine if there is wide acceptance of these recommendations." Consumer Watchdog cannot determine from the information CalOHII has provided what the recommendations would do and the reasons making them. Without that analysis it is impossible to say whether we could possibly support them. There are troubling basic procedural aspects about the harmonization process as well. Who selected the Privacy and Security Teams and under what authority? Though the Privacy Steering Team apparently has been meeting since February, your website says, "Privacy Steering Team Charter (Coming Soon)." Were votes taken at the meetings? I could find no record of them, nor any real minutes.

Another troubling aspect of the Privacy Steering Team recommendation is the concept of "adopting" HIPAA definitions. What exactly does it mean to "adopt" a HIPAA definition or rule? Does it mean to substitute the language and content of HIPAA for the language and content of each comparable California law for which the recommendation is to "adopt?" Is it the meaning of a HIPAA rule as currently set by federal courts? Since "adopt" is the operative verb and the fundamental purpose of harmonization, a clear understanding of its meaning and implications is essential.

Moreover, does adopting HIPAA into the CMIA diminish or eliminate California's authority over its health care privacy laws? Consumer Watchdog is concerned that by adopting HIPAA, California will be ceding authority to bureaucrats in Washington to determine the meaning of California law. This abandons one of the key strengths of HIPAA: non-preemption of more privacy-protective state laws. Will adoption of HIPAA provisions cede authority to federal courts to determine what California statutes mean? To be blunt, there is nothing about the process of developing these recommendations so far that leads Consumer Watchdog to believe that the goal is to strengthen privacy protections for Californians' medical information. We fear that greater consideration has been given to enabling adoption of Health Information Exchanges by providers and payers, than to the impact of the Exchanges on the privacy of individuals. Patient trust is critical to acceptance of HIE, because of the great sensitivity of individual health information. Consumer Watchdog believes that the current law harmonization process has done nothing to promote the public's trust. If anything, trust has been undermined. The very real risk is that harmonization will be a closed-door, industry-dominated process that lacks both political legitimacy and policy rationality.

CalOHII needs more transparency and accountability if it wishes to claim with confidence that these recommendations have public support. The federal government offers a model of how such a process could work. Under the federal Administrative Procedure Act's notice-and comment rulemaking provisions, federal agencies develop new rules on a concrete administrative record that includes not only the agency's own research and thinking, but also the written views of stakeholders, who themselves can introduce facts, experience and opinion. This process, which yielded HIPAA's Privacy and Security Rules, requires the agency to make its decisions based on a factual record, to consider and respond to public comments, and to articulate why the agency made important choices, thus promoting rational policy over political interest. You should follow a similar formal process for California's HIPAA harmonization efforts. We hope that these comments will lead to a transparent process that truly protects Californians' medical privacy as the harmonization effort goes forward.

Public Comments Received Regarding Law Harmonization Recommendations

Consumers Union and CDT

Members of the Privacy Steering Team, the Security Steering Team, and the California Office of Health Information Integrity:

Consumers Union and the Center for Democracy & Technology provide comment on the Privacy and Security Steering Teams' Law Harmonization Recommendations.

Last year, before CDT became a member, the PST embarked on an effort intended to harmonize the Health Insurance Portability and Accountability Act (HIPAA) and the Confidentiality of Medical Information Act (CMIA) in order to reduce actual and perceived conflicts, confusion, and inconsistencies presented by the two sets of health privacy standards. The PST's plan is to submit final recommendations to CalOHII, who will then submit them to the state legislature as a proposed amendment to the CMIA.

CU and CDT strongly support efforts to make privacy and security policy in California clearer and more comprehensive. Such efforts are critical to securing public trust in the use of HIT to improve individual and population health.

However, we share some of the concerns expressed by other consumer and privacy advocates about the harmonization project. As explained in more detail below, we believe the project will achieve its goals only if it is more focused and more transparent to the public.

CU and CDT are troubled by insufficient public transparency about the initiative and the significantly limited opportunities for input by other stakeholders. While the PST's meetings are available on webcast, the PST has not done an effective job of ensuring that a broad spectrum of stakeholders participates regularly in deliberations. By way of example, CDT, before being appointed to the PST, called in to several meetings and was often unable to follow the meeting due to both technical problems and a failure by the PST to make documents and drafts publicly available, either in advance of or during the meeting. In addition, the PST has not made all of its deliberations open to the public or available for public inspection and comment; nor have there been accessible, public announcements for the formation of "Task Groups" that the PST solicits for areas where specialized expertise is deemed important. As a result, important stakeholders, many of them seeing the draft recommendations for the first time, are confused about the intent of the recommendations and uncertain about their merit.

CU and CDT are also concerned that the current draft recommendations are not accompanied by clear explanations of the reasons supporting each recommendation. As a result, patients, consumers and other stakeholders do not have a clear understanding of the perceived need for the recommended change and consequently have limited information with which to evaluate it. As a simple example, we point to the definitional changes of the recommendations in the first phase of the harmonization project. The PST recommends adopting HIPAA's 'business associate' definition and removing the term 'contractor' that is currently used by the CMIA. However, the PST gives no explanation of the perceived need for the change; what if any benefits there would be to adopting the HIPAA business associate standard; which, if any, additional entities will now be regulated by the CMIA; and which, if any, entities may no longer be covered by the CMIA following the adoption of the new standard. Put simply - what would this change mean and how will it affect relevant stakeholders, especially patients and consumers? The HIPAA Privacy Rule and the CMIA have been working together in California for many years, for both paper-based and electronic exchanges of personal health information, so stakeholders need such explanations in order to evaluate the recommended changes.

CU and CDT believe that it is possible to refocus the harmonization initiative and build in sufficient public transparency and collaboration to ultimately achieve the worthwhile goals of the project, and as a new member of the PST, CDT is committed to helping to resolve these issues.

We suggest that PST refocus its efforts by more carefully examining existing privacy and security law in California and identifying clear gaps and areas of confusion that need to be addressed. This examination should be a public process, with opportunity for public comment, so that the ultimate "roadmap" for the harmonization process is one that has built and achieved broad public understanding and support. For example, the PST could initially consider addressing areas or issues for which there are currently no legal standards or safeguards for personal health information, or areas where current policies are not well understood or insufficiently enforced. Such policy gaps allow for the use and transfer of personal health information in ways that could undermine public trust, creating an environment where individuals do not feel safe or confident utilizing HIT tools. Specifically, CU and CDT believe the following issues could be the subject of focus by the PST:

- All business entities that access, use, and disclose personal health information should be held accountable for complying with comprehensive legal obligations to protect health data. Today, federal coverage under HIPAA is limited to traditional health care system entities (e.g., providers and insurers) and their

contractors (business associates). California lawmakers recently extended the CMIA's scope, but it is unclear whether these expansions suffice to provide comprehensive protections for consumers and patients regardless of which entity is accessing their information.

- Accountability for compliance with federal and state health privacy and security protections should be strengthened. Lack of effective enforcement of existing law undermines the public's trust in holders and users of personal health information. At the same time, enforcement policy at both federal and state levels must be robust without making health care entities so overly cautious that they fail to share information in ways that facilitate the provision of good health care, both at an individual and population level.
- Laws that protect electronic health data, such as the HIPAA Security Rule, should be reassessed to ensure that they are sufficient to meet new security challenges and to incorporate technological innovation. For example, reports of data breaches filed with the HHS Office for Civil Rights, which enforces the breach notification requirements under HIPAA, strongly suggest that entities covered by these rules are not consistently using encryption to protect stored health information. Encryption is one of the core protections that electronic health records and information exchange make available.
- Rules on the use of personal health information for marketing purposes should be strengthened. Survey data demonstrate that this remains a persistent concern of consumers. Congress enacted provisions in the HITECH Act to strengthen federal rules on the use of personal health information for marketing purposes, but two years later, regulations to implement those provisions have not been finalized and could instead weaken them.
- Policymakers should provide more clarity on how entities are expected to comply with existing and new health privacy laws. Entities that are uncertain about whether they can use and share information lawfully may err on the side of caution and decide not to share. In circumstances where sharing should be encouraged, such uncertainty could be an obstacle to progress in leveraging data to improve individual and population health.
- Policymakers should ensure that standards for de-identifying health data remain robust and should establish penalties for inappropriate or unauthorized re-identification.
- Where possible, data-sharing models that favor decentralization and local control should be prioritized in lieu of duplicate databases created each time health information is needed for a particular purpose. Duplication and centralization of data amplify the risk of security and privacy violations.

> Local control also builds upon existing infrastructures (augmented as necessary to adhere to privacy and security standards, to ensure interconnection and interoperability, and to incorporate innovations), so that the benefits of HIE are realized more quickly. (See "Achieving the Right Balance: Privacy and Security Policies to Support Electronic Health Information Exchange," California HealthCare Foundation Issue Brief (June 2012), written by Consumers Union and the Center for Democracy & Technology, http://www.chcf.org/publications/2012/06/achieving-right-balance)

As the PST and SST move forward with the harmonization process, it will be critical to be open and transparent at every step in the process. This includes providing detailed explanation of what legal standard each recommendation will specifically change, how the legal standard will be changed, and a justification or the rationale behind the recommendation. Including this additional information will allow patient/consumers, their advocates and the public the ability to formulate informed judgments on the changes, engage more significantly in the process, and feel confident that their privacy and security rights are being enhanced and not reduced.

Health information exchange should be built on institutional trust, bolstered by a comprehensive privacy and security framework that details clear policies regarding how data can be used and disclosed. The work PST is doing to build this framework should be continued. CDT is committed to helping the PST achieve a strong policy framework protecting health data.

We thank our fellow members of the PST, SST and CalOHII for the opportunity to issue these comments.

Public Comments Received Regarding Law Harmonization Recommendations

Dignity Health

On behalf of our 33 hospitals in California Dignity Health (formerly Catholic Healthcare West) appreciates the opportunity to submit comments on the CalOHII Privacy Steering Team's Law Harmonization recommendations. As the nation's fifth-largest non-profit hospital system, Dignity Health is committed to our mission of providing compassionate, high-quality care to all and strongly supports the use of Health Information Technology (HIT) as the central tool used to transform health care delivery. Dignity Health believes to achieve the true value of HIT hinges upon building public trust that health information will be kept private and secure and creating a consistent set of laws and regulations applicable to all those in California who use HIT to provide or pay for health care.

Dignity Health supports the effort to harmonize state and federal health information privacy law, and agrees consistent law will result in better patient care and will free-up resources with which to provide it. Inconsistency of state and federal health information laws presents a significant and well-recognized barrier to electronic health information exchange (HIE). Health care providers and HIE organizations alike find existing the law complicated, confusing, and inconsistent, and many chose not to participate because of it. CalOHII's efforts to make state and federal law consistent and to maintain strong privacy protections will allow HIE to flourish, creating a trust environment where providers will have better access to vital health information while enhancing patients' trust that their health information is protected.

Eliminating inconsistencies in federal and state privacy laws also creates consistent standards, reducing the need for policy analysts and compliance monitoring, redirecting scarce health care dollars toward direct patient care. While HIPAA's preemption rules are meant to work out conflicts between state and federal laws, such preemption rules are themselves complex and not easily understood by non-lawyers. In addition, the preemption rules do not work well when the inconsistencies are seemingly small and do not have obvious privacy implications. Those "small" inconsistencies occur with some frequency and have major operational implications. For example, California law requires that all valid patient authorization be printed in 14 point font. This state law is "more stringent" than HIPAA, according to the preemption rules, and thus must be followed. Unfortunately, the federal Social Security Administration has not complied with California law. Its otherwise-valid authorization forms are not printed in 14 point font, and so California providers who receive them have the difficult choice of either refusing to honor the authorization form (thus complying with the law but causing conflict with a federal agency and not helping the patient), or honoring the non-14-point form by producing the information requested (and thus violating California law but helping the patient who asked for the information to be sent to the Social Security Administration). Hospitals and physicians will be able to work more efficiently if such inconsistencies are eliminated through law harmonization, patients will benefit from increased legal clarity, and health care dollars can be put to their best, most productive use

While Dignity Health fully supports the effort to harmonize privacy law, we have specific concerns related to the proposal to add HIPAA provisions to California law. There are three specific problems with this proposal:

1) Multiple layers of enforcement. Unless legislation is drafted very carefully, adding HIPAA provisions into California law may mean that the state will be able (and perhaps required) to enforce the newly added provisions through investigation, imposition of penalties, and prosecution by state agencies. Thus, for violation of what used to be solely a HIPAA requirement—for example, the requirement to provide patients with a Notice of Privacy Practices—a physician or hospital might be penalized by both the Office for Civil Rights for the HIPAA violation, and by a state agency for violation of exactly the same provision as found in California law. In addition to the possibility of increased (doubled) penalties for hospitals and doctors, the addition of state enforcement of federal law could easily lead to inconsistent interpretations if state regulators do not investigate and enforce in ways fully consistent with the federal Office for Civil Rights, the current HIPAA enforcement agency.

   Many California providers already are subject to multiple enforcement and possible multiple penalties for a single privacy breach. Adding yet more state enforcement for violations already enforced by the federal government will not improve patient privacy protections and will add to the costs borne by California taxpayers Dignity Health believes the enforcement status quo must be maintained and urges CalOHII to ensure that California enforcement authority is not expanded beyond its current scope.

2) Future Inconsistencies. If the actual language of the HIPAA regulations is inserted word-for-word into California law, further inconsistencies between state and federal law will occur the minute the HIPAA regulations are amended. Dignity Health urges CalOHII to make clear throughout the legislative process its intent that California law and HIPAA continue to remain harmonized as the HIPAA regulations are amended. The need for such a statement of intent is heightened by the fact that as this comment is written, there are at least two federal Notices of Proposed Rule-Making (i.e., sets of amendments to the HIPAA privacy regulations) that will be issued soon in final form. It would be counterproductive to harmonize state and federal law in a way that permitted further inconsistencies when, as inevitably happens, laws or regulations are amended.

3) Individual Lawsuits. When Congress passed HIPAA in 1996, it chose not to permit individual lawsuits for HIPAA violations. Congress chose to have HIPAA requirements enforced by the federal Office for Civil Rights, the Department of Justice, and states' Attorneys General, but it deliberately chose not to allow individuals to sue for HIPAA violations. That decision, made by elected representatives, should be honored if HIPAA provisions are put into California law. California law does permit individuals to sue for state law privacy breaches, even if the individuals have suffered no harm. Private litigation, when added to an

already robust governmental enforcement environment, is costly, draining scarce resources from patient care. CalOHII should not add HIPAA provisions into California in such a way that violation of the newly-inserted HIPAA provisions can become the basis of private lawsuits. Dignity Health urges CalOHII to maintain the current litigation status quo as harmonization process moves forward.

Dignity Health appreciates the opportunity to respond to the Law Harmonization recommendations and hopes our input is helpful as CalOHII proceeds further.

Public Comments Received Regarding Law Harmonization Recommendations

American Civil Liberties Union of California, California Family Health Council, Electronic Frontier Foundation, Privacy Activism, Privacy Rights Clearinghouse, and World Privacy Forum

The American Civil Liberties Union of California, California Family Health Council, Electronic Frontier Foundation, Privacy Activism, Privacy Rights Clearinghouse, and World Privacy Forum submit the following comments on the California Office of Health Information Integrity (Cal-OHII) Privacy and Security Steering Team's Law Harmonization Recommendations.

1. **Introduction**

We generally support Cal-OHII's goal of clarifying health privacy laws and making them more accessible to all California stakeholders. We recognize that California law in this area is scattered across many code sections and poorly mapped to HIPAA. Our concern, however, is that the current harmonization process is both substantively and procedurally risky. The main substantive risk is that harmonization will weaken existing privacy protections, forgo an important opportunity to strengthen privacy protections, or freeze the law so as to make it harder for California to respond to the privacy challenges of new health IT.

The procedural risks are closely related. Precisely because health privacy law is so complex, it is difficult for consumer and privacy advocates to fully understand the costs and consequences of harmonization. Even the Electronic Frontier Foundation (EFF), which has been part of the harmonization process, has found it difficult to explain and justify the harmonization recommendations to fellow consumer and privacy groups.

Cal-OHII needs more transparency and accountability if it wishes to claim with confidence that these recommendations have public support. For instance, under the federal Administrative Procedure Act's notice-and-comment rulemaking provisions, federal agencies develop new rules on a concrete administrative record that includes not only the agency's own research and thinking but also the written views of stakeholders, who themselves can introduce facts, experience and opinion. This process, which yielded HIPAA's Privacy and Security Rules, requires the agency to make its decisions based on a factual record, to consider and respond to public comments, and to articulate why the agency made important choices, thus promoting rational policy over political interest. We need a similar formal process for HIPAA harmonization efforts.

2. **The Law Harmonization Recommendations document and the process by which it was arrived at are opaque**.

- **The section "Why Is the Change Needed?," which purports to explain the purpose of reconciling HIPAA and the CMIA, is either tautological or unclear.** The Privacy Steering Team (PST) states that it is concerned about the

impact of new technologies on "consumer privacy and provider liability . . that existing laws were never originally created to address." Resolving the discrepancies between HIPAA and the CMIA will, supposedly, solve the problem.

We do not disagree that there are discrepancies between state and federal laws regarding the privacy and security of protected health information. Nor do we disagree that the law needs to be updated to address technological change. What the PST Law Harmonization Recommendations fail to explain, however, is *how* harmonization solves the problems that universal electronic health records will create. It also fails to explain why bringing California laws in line with HIPAA is preferable to creating stronger protections for Californians' medical records. Essentially, the document seems to say that harmonization is needed because it is needed.

- **The Law Harmonization Recommendations are not understandable to advocates or members of the public in their current form, and a great deal more explanation is needed.** The recommendations do not explain the meaning of the laws and regulations the PST intends to harmonize—neither the HIPAA sections nor the corresponding sections of the CMIA. The document does not explain how or why the PST arrived at its recommendations.

Perhaps most important, the PST does not explain in detail the consequences of harmonizing HIPAA and the CMIA to Californians. That is, what privacy standards will apply to their medical records and whether and how they will benefit from harmonization—or not. This is a question that needs to be answered, since HIPAA was conceived as a baseline of privacy protections and specifically does not pre-empt stronger state laws, like California's. We need clearer and better documented assurances that harmonization will not subtly undermine rights and remedies under existing law. We need litigation analyses to convince us that changes will not affect the ability of Californians to hold covered entities accountable. We observe that HIPAA provides no remedies to individuals at all.

One possible addition to the harmonization document could include a column that indicated whether the proposed change was "more protective" or "less protective" in relation to current California privacy law, with an explanation of each determination in an appendix. This is one example, but there are different ways the harmonization document could be made more understandable and comprehensive.

Along with addressing the question of the benefits of harmonization to individuals, the PST should be forthcoming about other beneficiaries. Is harmonization intended to benefit individuals, or is its primary purpose to remove the privacy "barriers" to the flow and uses of electronic PHI?

- **The harmonization process up to this point is poorly conceived.** Medical privacy at the beginning of widespread adoption of HIE is a critical issue. The laws that regulate it should not be developed in the dark. The PST's intentions regarding harmonization are unclear. Does the PST believe it is necessary simply because there are discrepancies between HIPAA and the CMIA? Because other states are doing it? Is the purpose to pave over differences between HIPAA and the CMIA and eliminate privacy "barriers" to HIE?

The lack of clarity about the PST's operations and intentions does not encourage public participation. Nor does the absence of clear, point-by-point explanations of the content of sections of HIPAA and the CMIA, along with the reasons the PST believes they should be harmonized and the consequences of harmonization. As a privacy advocate member of the PST, EFF readily admits that it has relied heavily on analysis of both state and federal law provided by both Cal-OHII staff, information provided by legal and practical experts on the PST, and information from invited subject-matter experts. EFF has also seen firsthand that reasonable lawyers and experts often disagree about the meaning of California law and how it intersects with HIPAA.

Up to now, the PST has done little to encourage public participation, nor has it provided the information the public needs to make that participation meaningful.

3. **What is the goal of harmonization?**

- **Do no harm.** It is our understanding that HIPAA–CMIA harmonization is *not* intended to weaken existing privacy protections in California law. We nevertheless fear that harmonization may have the opposite effect of bringing California standards down to the HIPAA level and filling omissions in California law with weak HIPAA regulations. It is not possible to know from the PST's harmonization narrative what it has done to ensure that its recommendations do not weaken state law privacy protections.

For example, Article I, Section 1 of the California constitution is a bulwark of state privacy law, but it is not clear that the PST did any constitutional analysis in arriving at its harmonization recommendations. Consider the recommendation to adopt the HIPAA provision at 45 C.F.R. § 164.512(k)(2):

> (2) National security and intelligence activities. A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, et seq.) and implementing authority (e.g., Executive Order 12333).

This provision appears to allow any covered entity to disclose any health record to the CIA, FBI, NSA, and many other federal agencies that play a role in intelligence, counter-intelligence, and national security activities without a court

order, without any procedural or substantive protections or barriers, and even without any request from the agency. Under this provision, a hospital could disclose any or all of its patient medical records to the CIA on the hospital's own initiative. A hospital could even allow the CIA or other federal agencies to access the hospital's health record system on a permanent basis.

Why is this recommended? How did the PST determine that existing law permitted this permissive disclosure? Did the PST consider whether the state constitutional right to privacy requires greater protections? Did it consider whether California should allow these disclosures without any standard or procedure—like a subpoena—to protect the privacy interests of patient? Because existing California law is more privacy-protective overall than HIPAA, the spirit of California law would be better served by a more privacy-protective approach to national security or intelligence disclosures— even if nothing in the letter of California law currently does so. We add that we perceive no benefit to either California patients or the promotion of HIE if this HIPAA provision is adopted.

Another example is the marketing provisions of HIPAA, as amended by HITECH. Neither HIPAA nor the CMIA is a model of clarity on what "marketing" means, and what is or is not permitted. The PST's narrative document adopts the HIPAA marketing rule. Are we to assume that it also adopts HITECH's changes to the marketing rule? If the recommendation is to adopt, where is the discussion of how HIPAA + HITECH is either equivalent to or better than the CMIA? Where is the analysis of whether the new—and not yet final—federal rules will restrict marketing or will actually allow more of it?

Both of these examples are simply examples, but they lead us to worry about the harmonization project generally. Part of the issue may be viewed as a tension between fidelity to text and fidelity of intent, most clearly expressed in state constitutional privacy law. Precisely because we expect that the growing use of EHR and HIE exposes more patient data to more entities, and thus to more privacy and security risk, we believe fidelity of intent is appropriate.

That the recommendations may ultimately be translated into potential legislative language only heightens our concern. We have all worked on legislation, and we all know that good policy ideas can mutate greatly in a political process. In this context, clear and detailed documentation is necessary protection.

4. **What does it mean to "adopt" HIPAA?**

- **The recommendations do not explain what it means to "adopt" HIPAA.** The recommendations use the term "adopt" throughout, but do not explain what it means to adopt a HIPAA definition or rule. Does it mean to substitute the language and content of HIPAA for the language and content of each comparable California law for which the recommendation is to "adopt?" Is it the meaning of a HIPAA rule as currently set by federal courts? Since "adopt" is the

operative verb and the fundamental purpose of harmonization, a clear understanding of its meaning and implications is essential.

- **Does adopting HIPAA into the CMIA diminish or eliminate California's authority over its health care privacy laws?** We're concerned that by adopting HIPAA, California will be ceding authority to bureaucrats in Washington to determine the meaning of California law. This abandons one of the key strengths of HIPAA: non-preemption of more privacy-protective state laws. Will adoption of HIPAA provisions cede authority to federal courts to determine what California statutes mean?

Does harmonization make it harder for California to craft rules that are stronger than federal law? California has consistently been a policy leader on individual privacy; for example, it was the first state to have a data breach law and the first to apply it to medical records. Once harmonization is accomplished, will California be unwilling to rock the harmony boat and address new privacy concerns that emerge after HIE has been implemented?

Consider one area where HIE could make it desirable to develop new law where none currently exists: re-identification of de-identified data. Leaving aside research-supported doubts about how de-identified such data actually is, it seems likely that as EHRs make enormous volumes of patient data easily accessible, demands for de-identified data for purposes we have yet to imagine will increase. Even current uses of de-identified data highlight the need to regulate re-identification. For example, some companies currently offer free EHR systems to doctors—a business model supported by monetizing de-identified data culled from those EHRs.

Another example is the business of drug detailing reports, sold to pharmaceutical companies by data miners like IMS, to assist drug salesmen in targeting doctors based on knowledge of their prescribing habits. IMS takes data that is encrypted by applications that IMS installs at the data source. IMS removes the identifying elements, but the data is still identified by a number and could therefore be easily re-identified. A patient's activities can be tracked over time to show other prescriptions filled for the number assigned to that patient, how long the patient takes a drug, and if a drug is discontinued or a new one prescribed. What IMS does to de-identify prescription data is apparently enough to satisfy HIPAA, as long as IMS obtains an expert's determination that the risk of individual identification is very small (very small is not defined). The HIPAA rule on this point uses very poorly defined standards. It opens the door to exploitation of patient records under a scheme where privacy protections rest on the opinion of an expert hired by those seeking to exploit those records.

If such practices continue and expand, a California policy that protects individuals from "de-identification" that still allows continuous tracking and that also strongly restricts re-identification, would be a good idea. Merely requiring entities to publicly disclose their de-identification methodology and their expert's analysis of the risk of individual identification could improve matters considerably. But would a post-harmonization California be willing to enact a regulation that exceeds HIPAA requirements? For that matter, would a post-harmonization California even contemplate a far more fundamental shift in the data management paradigm: enhancing individual privacy by adopting technologies that enable personal control and management of medical information, as opposed to control by institutions and organizations?

5. **Does harmonization take into account the changes that HITECH will make once the new regulations are published?**

- **HITECH is not mentioned in the narrative.** Are we to assume that whatever changes HITECH makes to HIPAA will simply be absorbed into the HIPAA rules that the PST recommends adopting?

6. **Conclusion**

In general, we are not reassured that either the process of developing these recommendations so far, or the goal of the process, is to strengthen privacy protections for Californians' medical information. We fear that greater consideration has been given to enabling adoption of HIE by providers and payers, than to the impact of HIE on the privacy of individuals.

Patient trust is critical to acceptance of HIE, because of the great sensitivity of individual health information. We believe that the current law harmonization process does a poor job of promoting public trust. The very real risk, from a consumer/patient perspective, is that harmonization will be a closed-door, industry-dominated process that lacks both political legitimacy and policy rationality. We hope that these comments will help improve that process going forward.

Public Comments Received Regarding Law Harmonization Recommendations

Kaiser Permanente

Kaiser Permanente[1] appreciates the opportunity to offer comments on CalOHII's Law Harmonization Recommendations ("Recommendations"). We recognize the substantial efforts of the Privacy and Security Steering Team ("Steering Team") to harmonize provisions of California's Confidentiality of Medical Information Act ("CMIA") with the federal Health Insurance Portability and Accountability Act ("HIPAA") in order to provide more consistency in California law related to medical information privacy and security. We generally support the approach recommended by the Steering Team.

Kaiser Permanente addresses these issues from our perspective as an integrated care delivery system and a leader in health information technology. As part of our commitment to the highest quality care, Kaiser Permanente has made a significant investment in developing a secure Electronic Health Record ("EHR") system, KP HealthConnect®. We are strongly committed to facilitating the development of health information exchange to enhance patient care and improve the health of the communities we serve.

General Comments

In general, we support the Steering Team's efforts to align CMIA with HIPAA.

2

This first set of Recommendations begins to address existing fragmentation of California privacy law by harmonizing definitions between CMIA and HIPAA. We agree that HIPAA is a reasonable starting point for evaluating and addressing gaps or deficiencies in current California law. With HIPAA as the framework, analysis of existing California law should be fairly comprehensive and proceed from common understanding of key terms and requirements.

However, with significant HIPAA revisions pending, we recommend that CalOHII consider how to "adopt" HIPAA definitions to avoid further inconsistency and confusion. Incorporating a specific version of HIPAA would be counterproductive to harmonization.

We have also addressed concerns with specific recommendations on definitions:

Item 23 'Health care'

The comment suggests considering including medical supply sales in the definition of health care; however, HIPAA already includes the sale of prescribed devices and medical supplies in the definition.

Item 26 'Health Care Provider'

The comment states that this substitution of the HIPAA definition for the current CMIA definition "is not intended to expand the breach notification requirements." The comment does not clearly state whether the recommendations are referencing the Federal Breach

notification requirements or state laws, specifically Health & Safety Code 1280.15; or Civil Code 1798.82.

Item 27 'Health Information'
While the change may exclude certain information created by pharmaceutical manufacturers (because they are not HIPAA-covered entities), it will not remove protections for information collected or accessed by pharmaceutical manufacturers from HIPAA-covered entities.

Item 34 'Individually identifiable health information'
We reiterate our concern about the reference to breach notification (see *Item 26* comment, above)

Item 40 'Organized Health Care Arrangement'
Generally we would oppose any California revisions to the HIPAA definitions or provisions for organized health care arrangements ("OHCA").

Comment #1, that an OHCA should "[g]enerate [a]…list of participants in the OHCA in the Notice of Privacy Practices" ("NPP") is confusing and restrictive. HIPAA allows OHCA participants to use either a joint NPP or separate NPPs. If the OHCA opts for a joint notice, it should describe "with reasonable specificity the covered entities, or class of entities, to which the joint notice applies." (*See* 45 CFR 164.520 (d)(2)(i)). We recommend maintaining the flexibility and clarity afforded by current HIPAA provisions and not to compel an OHCA to use a joint NPP or require participants to revise their separate NPPs to list other OHCA participants.

HIPAA-covered entities that already operate as OHCA participants should not be required to meet documentation requirements above and beyond what is already required for OHCA under HIPAA (Comment #2).

It is not clear whether Comment #3, which suggests "[a] consistent mechanism of transparency which addresses the literacy of the consumer so it is easily understood," refers generally to NPPs or specifically to OHCAs.

Comment #4 ("Consider implementing an oversight mechanism within each OHCA - keeping in mind other oversight entities activities so as to prevent conflict") does not clearly explain what it means by "oversight mechanism" and therefore, it raises serious concerns that California law could require OHCAs to develop additional levels of bureaucracy, possibly with overlapping accountabilities. We oppose altering or augmenting the definition of OHCA to increase administrative burdens for participants, without compelling evidence that such changes will provide greater benefit to consumers. The oversight mechanism is especially unnecessary where individual OCHA participants are subject to central oversight, often by a single parent organization with directors or trustees already charged with fiduciary responsibilities. In such

circumstances, the oversight mechanism would be redundant at best, with the potential to stifle flexibility and creativity.

Item 67'Minimum necessary requirements'

We strongly urge CalOHII to ensure that California law aligns closely with HIPAA's definition and application of the minimum necessary standard, especially as it concerns sharing of information among treating providers, which has important patient safety and health care quality implications. The preservation of treatment flexibility is also critical for the development of health information exchange ("HIE") networks, where most activity is for purposes of treatment, and often conducted under exigent circumstances where complex restrictions are difficult to interpret. We also agree with HIPAA's approach that provides reasonable discretion to covered entities in applying the standard.

Item 87 'Requirements for organized health care arrangements'

See our comments in response to *Item 40*, above.

Item 90 'Access to patient's information'

In "ensuring to explicitly include HIEs/HIOs," we recommend that CalOHII should distinguish an exchange that merely routes protected health information ("PHI") directly from one entity/provider to another, also defined as "directed" or "point-to-point" exchange. In those instances, details about the patient's identity, data content, etc. of the exchange will not be known or recorded by the Health Information Organization ("HIO") via the HIE. As 4 recommended by the "Privacy and Security Tiger Team" established by the Office of the National Coordinator for Health IT, U.S. Department of Health & Human Services,2 we believe it is appropriate to distinguish (a) HIOs that retain or host PHI or otherwise control access to PHI, from (b) directed (or point-to-point) exchanges that do not involve access to or storage of PHI by a third party HIO.

Item 96 'Accounting of Disclosures'

This Item is an example of why changes to CMIA should avoid adopting a specific version of HIPAA. HIPAA requirements for Accounting of Disclosures are subject to revision under HITECH, final rules still pending.

Items 105 to 110 (Security Standards & Requirements)

We are concerned about recommendations to expand requirements drafted specifically for the HIE Demonstration Project. While those regulations were subject to public comment, they are also narrow in scope and should not be expanded to broader applicability without revision. For instance, these items apply to an "Entity," a term undefined in either HIPAA or CMIA.

We recommend adopting security provisions in HIPAA, which impose risk assessment and remediation responsibility on covered entities, but permit flexibility to adapt security practices to organizational circumstances and characteristics.

We also recommend ensuring that these requirements align with the standards and requirements for the federal EHR Incentives program under CMS (i.e., “Meaningful Use”), which establishes (or has proposed) certain security measures for EHRs.

Conclusion

We appreciate your willingness to consider our comments.

Public Comments Received Regarding Law Harmonization Recommendations

Privacy Rights Clearinghouse

Introduction

The Privacy Rights Clearinghouse (PRC) appreciates the opportunity to submit comments to the California Office of Health Information Integrity (CalOHII) regarding the proposed harmonization of California's Confidentiality of Medical Information Act (CMIA) with the federal Health Insurance Portability and Accountability Act (HIPAA).[1]

The PRC is a nonprofit organization with a two-part mission: consumer education and consumer advocacy. The organization, which was established in 1992, is based in San Diego, California, and serves Californians as well as consumers nationwide. The PRC has invited individuals' complaints and questions since its inception nearly 20 years ago. (Website: www.privacyrights.org)

Over the years, consumers' complaints and questions to the PRC have spanned a broad spectrum of informational privacy issues, including: identity theft, telemarketing, financial privacy, credit reporting, children's online safety and privacy, online privacy, public records, telephone and telecommunications privacy, and last but not least, medical privacy. In fact, medical privacy is among the top issues on the PRC's hotline and has been since the PRC was established 20 years ago.

Discussion

The PRC is among several organizations that has signed onto the Electronic Frontier Foundation' comments to CalOHII. We are also submitting the following comments separately in order to underscore our concern that the harmonization process, as currently structured, could weaken the CMIA.

California's medical privacy law is among the strongest state medical privacy measures in the nation. Long-time privacy historian and publisher Robert Ellis Smith (*Privacy Journal)* has analyzed privacy laws in the 50 states in his compendium, *Compilation of State and Federal Privacy Laws.* He ranks California highest in overall privacy protection.[2] Key among California's privacy-related laws is the California Medical Information Act.

HIPAA serves as a floor and not a ceiling. States can have health privacy laws that are stronger than HIPAA, and California is an example of a state with stronger laws. Californians would be ill-served by a harmonization process that, with the best of intentions, would result in undermining the CMIA and weakening medical privacy protection for residents of the state.

We have examined the table that has been prepared by CalOHII (as initially developed by CHILI) and is included in the 33-page document, *Privacy and Security Steering Team Law Harmonization Recommendations*.3 The table that begins on page four is impressive, and is well structured – with sections on Definitions, Uses and Disclosures, Organizational Requirements, Patient Rights, Compliance, and Security Standards.

But the recommendations as currently written and formatted in this table do not function to foster deep understanding of the proposed harmonization process. We believe the table could and should go further.

The Electronic Frontier Foundation suggests that a column be added to the table which indicates whether the recommendation would strengthen or weaken the CMIA. We strongly endorse this suggestion. As written, this document is difficult to grasp, even for those like myself who have worked in the privacy arena for a long time.

We would also recommend that web-links be built into the table that enable users to link online to *specific subsections* of both the California and federal law. What both CHILI and CalOHII have done with this table is to create a tool to serve as a foundation for analysis and discussion of the proposed harmonization process. We believe that enhancing this tool, as suggested above, will better enable individuals – including policymakers, agency staff, consumer advocates, healthcare professionals, and interested individuals -- to understand the recommendations that have been proposed.

Healthcare institutions are ramping up their adoption of electronic medical records (EMR) systems, including the development of health information exchange systems (HIE). Many such endeavors are funded by grants from the American Recovery and Reinvestment Act of 2009 (ARRA).

Experts tout the many benefits of the adoption of EMRs and the establishment of HIEs. The CalOHII harmonization document states that “harmonizing California privacy and security laws is critical to the successful implementation of health information exchange (HIE) in California.”4 Brief mention is made of minimizing confusion and enabling the “safe and secure exchange of personal health information.”

But this section of the harmonization document lacks the in-depth discussion that is needed to explain why harmonization is so essential to HIE – as well as a parallel discussion of the increased risks of data breaches that can accompany both the adoption of EMRs and the establishment of HIEs.

We believe a richer analysis is required in the section titled “Why Is the Change Needed” before embarking on a harmonization process, especially when the result could be the weakening of health privacy protections in law.

We realize that the recommendations in this document may ultimately be used as the source documentation to draft state legislation regarding harmonization. Without a much clearer exposition of *why* harmonization is needed and *how* it should be structured, we can only expect such legislation to be ill-conceived.
The legislation process is complex and unpredictable. If the source documentation that launches a legislative endeavor is difficult to comprehend and lacks a clearly stated overriding purpose and goals, we cannot expect the legislative outcome to be good public policy.

Conclusion

A harmonization process that has the unintended consequences of weakening California health privacy law is not in the best interests of the residents of this state.

We urge CalOHII to strengthen the documentation that will be used by stakeholders to evaluate the harmonization process and determine what the true impact of harmonization would be on California law.

As written and formatted now, the *Privacy and Security Steering Team Law Harmonization Recommendations* is of use only to the cognoscenti. If harmonization goes forward, it is not only critical that the decision process be guided by robust and understandable documentation, but also that the interests of consumers and patients be given the highest priority.

Thank you for your consideration of these comments.

Seyfarth Shaw LLP

Thank you for the opportunity to submit written input relevant to your review and study of the impact of harmonizing CMIA with HIPAA. My name is Nanette Zamost. I am a partner in the Employee Benefits Group of the law firm of Seyfarth Shaw LLP. Our firm represents a number of multiemployer Taft Hartley health and welfare funds, ranging in size from small regional funds to some of the largest collectively bargained plans in California and throughout the U.S. These funds are not insurers or traditional medical groups. Rather, they are not-for-profit ERISA welfare plans, jointly administered by contributing employers and unions to provide health benefits for the employers' employees/unions' members and their eligible dependents ("participants"). Especially in this time of rising costs and changing laws, our clients are dealing with the challenges of providing good, cost-effective health care benefits for their participants.

I welcome the efforts of CalOHII and the Steering Teams to harmonize CMIA with HIPAA. Unfortunately, a collateral effect of the disconnect between these federal and state laws has been to create roadblocks to implementation of proven cost-effective and results-oriented programs to help the health of fund participants. ERISA welfare plans are HIPAA Covered Entities (health plans), entitled to information about their own participants for the HIPAA-sanctioned purposes of treatment, health care operations, and payment. However, the different definitions and provisions under CMIA can make health care providers and other entities subject to CMIA reluctant to provide data to ERISA plans about their own participants, even though these entities agree that the plans are clearly entitled to the information under HIPAA. As a result, these perceived gaps can interfere, for example, with efforts of health plans who need access to participant data in order to establish meaningful disease management programs and other valuable health services.

While recognizing the importance of individuals' privacy interests, I urge you to also keep in mind the valuable health care delivery opportunities which would be served by harmonizing these laws in all aspects relevant to provide disclosure/access to HIPAA Covered Entities for proper HIPAA purposes.

Thank you.